



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/973,447	10/09/2001	Edward R. Rowe	07844-448001	7875

21876 7590 08/19/2005

FISH & RICHARDSON P.C.
P.O. Box 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 08/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center">Office Action Summary</p>	<p>Application No.</p> <p>09/973,447</p>	<p>Applicant(s)</p> <p>ROWE, EDWARD R.</p>	
	<p>Examiner</p> <p>Jung W. Kim</p>	<p>Art Unit</p> <p>2132</p>	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 February 2002 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| <p>1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)</p> <p>2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)</p> <p>3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date <u>9/02</u>.</p> | <p>4) <input type="checkbox"/> Interview Summary (PTO-413)
 Paper No(s)/Mail Date. ____.</p> <p>5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)</p> <p>6) <input type="checkbox"/> Other: ____.</p> |
|--|---|

Handwritten mark

DETAILED ACTION

1. Claims 1-36 are pending.

Information Disclosure Statement

2. The items listed on the Information Disclosure Statement (IDS) filed September 3, 2002 has been considered.

Drawings

3. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings are informal. All drawings must be made by a process which will give them satisfactory reproduction characteristics. Every line, number, and letter must be durable, clean, black, sufficiently dense and dark, and uniformly thick and well-defined. 37 CFR 1.84. Applicant is advised to employ the services of a competent patent draftsman outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The drawings are adequate for prosecution, but new drawings will be required at the time of allowance.

Claim Objections

4. Claims 32 and 36 are objected to because of the following informalities: on line 7 of the respective claims, replace "single skeleton" with "single skeleton key".

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claim 2 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 2 recites the limitation of storing the encrypted document decryption key in the document; however the specification only discloses storing the encrypted document decryption key in the encrypted document (see Specification, pg. 3, last paragraph).

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
9. Claim 1 recites the limitation "the document" in line 7. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-36 are rejected under 35 U.S.C. 101 because the claims are not limited to tangible embodiments. In view of Applicant's disclosure, specification pg. 20, lines 7-9, the medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (e.g., hardware implemented) and intangible embodiments (e.g., software, propagated signal). As such the claims are not limited to statutory subject matter and is therefore non-statutory.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000.

Art Unit: 2132

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

12. Claims 1, 2, 8, 10, 13, 23-25 and 34 are rejected under 35 U.S.C. 102(e) as being anticipated by Takeda et al. USPN 6,336,189 (hereinafter Takeda '189).

13. As per claim 1, Takeda '189 discloses a method for managing access to electronic documents, comprising:

- a. associating a first key with an encrypted document decryption key, the encrypted document decryption key being associated with an encrypted document, the encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the document, the first key being usable to decrypt the encrypted document decryption key (col. 4:52-5:52, especially 5:1-5); and
- b. providing the first key in an access controlled manner to users for use in opening the document (5:20-24).

14. As per claim 2, the rejection of claim 1 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the method further comprising storing the encrypted document decryption key in the document (figs. 1 and 6).

Art Unit: 2132

15. As per claim 8, the rejection of claim 1 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the step of providing the first key in an access controlled manner comprises sending the first key to users in rights management information specific to system of the users to whom the first key is sent (fig. 6, reference no. 200).

16. As per claim 10, the rejection of claim 1 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the step of providing the first key in an access controlled manner comprises sending information used to synthesize the first key in rights management information (col. 5:15-34).

17. As per claim 13, the rejection of claim 1 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the method further comprising providing a document decryption key in an access controlled manner to users for accessing the document without using the first key (col. 5:15-25).

18. As per claims 23 and 24, the rejection of claim 1 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the encryption and decryption of the document encryption key uses public key encryption (col. 5:1-45). The aforementioned cover the limitations of claims 23 and 24.

19. As per claim 25, the rejection of claim 24 under 35 U.S.C. 102(e) is incorporated herein. (supra) In addition, the step of providing the first key in an access controlled

Art Unit: 2132

manner comprises sending information used to synthesize the first key in a rights management file and wherein the rights management file enables access to the private key (col. 5:15-34).

20. As per claim 34, it is a claim corresponding to claim 1 and it does not teach or define above the information claimed in claim 1. Therefore, claim 34 is rejected as being anticipated by Takeda '189 for the same reasons set forth in the rejection of claim 1.

Claim Rejections - 35 USC § 103

21. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

22. Claims 3-7, 11, 32, 33 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takeda '189 in view of Richards USPN 6,069,957 (hereinafter Richards '957).

23. As per claim 3, the rejection of claim 1 under 35 U.S.C. 102(e) is incorporated herein. (supra) Takeda '189 does not disclose encrypting the first key and associating a second key with the encrypted first key, such that the second key is used to decrypt

the encrypted first key. Richards '957 discloses restricting access to programs whereby program material is encrypted using a key hierarchy, or "key-upon-key" encryption (col. 1:25-30), including the steps of:

- c. encrypting a first key usable to decrypt a program decryption key, which is usable to decrypt a program (9:14-15);
- d. associating with the encrypted first key a second key that can be used to decrypt the encrypted first key (9:16-17); and
- e. providing the second key in an access controlled manner to users for use in opening all documents that can be opened through use of the first key (10:34-63).

It would be obvious to one of ordinary skill in the art at the time the invention was made to combine the "key-upon-key" encryption technique in the invention of Takeda '189 since it decouples the step of securing the data-decrypting key and the user's private key, and it is desirous to reduce the complexity and overhead of key management to maintain secure and updated key values. Richards '957, 10:5-12. The aforementioned cover the limitations of claim 3.

24. As per claims 4-7, the rejection of claim 3 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Richards '957 discloses using more than one data decryption key for a given program, using a different data decryption key for a different program (col. 8:36-48). Hence, the method further comprising:

- f. providing a second encrypted document decryption key for a second encrypted document, the second encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the second encrypted document decryption key being encrypted so that the first key is usable to decrypt the second encrypted document decryption key, and associating the first key with the second encrypted document decryption key (8:36-48; 9:12-10:63; 'SK' is encrypted by either 'PK' or customer_code);
- g. providing a third encrypted document decryption key for the second encrypted document, the third encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the third encrypted document decryption key being encrypted so that a third key is usable to decrypt the third encrypted document decryption key, associating the third key with the third encrypted document decryption key, and providing the third key in an access controlled manner to users for use in opening the second document (8:44);
- h. associating a third key with a second encrypted document decryption key for a second document, the second encrypted document decryption key when decrypted yielding a document decryption key usable to decrypt the second document, the second encrypted document decryption key being encrypted so that the third key is usable to decrypt the second encrypted document decryption key; encrypting the third key, associating the second key with the encrypted third key, the second key being usable to decrypt the encrypted third key, and

providing the second key in an access controlled manner to users for use in opening all documents that can be opened through use of the third key (8:44; 9:12-10:63).

25. As per claim 11, the rejection of claim 3 under 35 U.S.C. 103(a) is incorporated herein. (supra) Although Takeda '189 does not expressly disclose the encrypted first key is stored in a rights management file, it is notoriously well known in the art for digital information to be stored in memory within a data file, since files enable an efficient organizational storage means. Examiner takes Official Notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the rights management information to comprise a rights management file since it is desirable to store digital information conforming to a conventional file system. The aforementioned cover the limitations of claim 11.

26. As per claims 32, 33 and 36, the rejection of claim 3 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, a single skeleton key can be used to open multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys (Richards '957, col. 7:24-33; 8:44-64; 9:12-18). The aforementioned cover the limitations of claims 32, 33 and 36.

27. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Takeda '189 in view of Richards '957, and further in view of Stallings, Cryptography and Network Security, Section 12.1 "Pretty Good Privacy" (hereinafter Stallings).

28. As per claim 12, the rejection of claim 11 under 35 U.S.C. 103(a) is incorporated herein. (supra) Takeda '189 does not expressly disclose associating a unique identifier with the second key and storing the unique identifier in the rights management information with the encrypted first key. Stallings discloses an overview of PGP security, which includes a key management scheme, wherein a key ID is assigned to a key-decrypting key for the purpose of efficiently identifying a key that decrypts an encrypted data decryption key (pg. 365, figure 12.3 and related text). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to utilize key identifiers for the purpose of associating key-decrypting keys to an encrypted data-decrypting key, since it is desirous to efficiently associate such decryption keys with their encrypted values. Stallings, pg. 364, 1st paragraph. The aforementioned cover the limitations of claim 12.

29. Claims 9 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takeda '189.

30. As per claim 9, the rejection of claim 8 under 35 U.S.C. 102(e) is incorporated herein. (supra) Although Takeda '189 does not expressly disclose the rights

Art Unit: 2132

management information comprises a rights management file, it is notoriously well known in the art for digital information to be stored in memory within a data file, since files enable an efficient organizational storage means. Examiner takes Official Notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the rights management information to comprise a rights management file since it is desirous to store digital information conforming to a conventional file system. The aforementioned cover the limitations of claim 9.

31. As per claim 16, the rejection of claim 10 under 35 U.S.C. 102(e) is incorporated herein. (supra) Takeda '189 does not expressly disclose the rights management information provides a license and defines a set of permission rights associated with the license. However, providing a license and defining permission rights based on the license is a notoriously well known feature in the art. Digital data for the purpose of mass distribution often includes a user's agreement as well as licensing limitations that defines the extent of operation of the digital data. Examiner takes Official Notice of this teaching. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Takeda '189 to provide a license and define a set of permission rights associated with the license, since it is desirous to limit use and access of a digital document to the owner's discretion. The aforementioned cover the limitations of claim 16.

Art Unit: 2132

32. Claims 14, 15, 17, 26-29 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takeda '189 in view of Stallings.

33. As per claims 14 and 15, the rejection of claim 2 under 35 U.S.C. 102(e) is incorporated herein. (supra) Takeda '189 does not expressly disclose associating a unique identifier with the first key, wherein the unique identifier is stored in the document in association with the encrypted document decryption key to associate the first key with the encrypted document decryption key. Stallings discloses an overview of PGP security, which includes a key management scheme, wherein a key ID is assigned to a key-decrypting key for the purpose of efficiently identifying a key that decrypts an encrypted data decryption key, wherein the key ID is stored with the message and encrypted data-decrypting key (pg. 365, figure 12.3 and related text). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to utilize key identifiers for the purpose of associating key-decrypting keys to an encrypted data decryption key, since it is desirous to efficiently associate such decryption keys with their encrypted values. Stallings, pg. 363, last paragraph-364, 1st paragraph. The aforementioned cover the limitations of claims 14 and 15.

34. As per claim 17, the rejection of claim 16 under 35 U.S.C. 103(a) is incorporated herein. (supra) Takeda '189 does not expressly disclose the set of permission rights specifies a right allowing another key to be associated with the rights management information so that a holder of such a key has access to the first key. Stallings

discloses an overview of PGP security, which includes a key management scheme, wherein a key ID is assigned to a public key for the purpose of efficiently identifying a key that decrypts an encrypted data decryption key, wherein the key ID is stored with the message and encrypted data-decrypting key (pg. 365, figure 12.3 and related text). This pairing of a key-encrypting key with an encrypted key establishes a right to access the encrypted key. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to utilize key identifiers for the purpose of associating key-decrypting keys to an encrypted data decryption key, since it is desirous to efficiently associate such decryption keys with their encrypted values. Stallings, pg. 363, last paragraph-pg. 364, 1st paragraph. The aforementioned cover the limitations of claim 17.

35. As per claim 26, Takeda '189 discloses a method for accessing an electronic document comprising:

- i. obtaining an encrypted electronic document (fig. 7, "Process of data capsule");
- j. obtaining a collection of keys, the keys including keys that are encrypted, the keys having associations between certain pairs of them, where each association of a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the

encrypted document, and where a user has access to and can use certain ones of the keys in the collection (col. 5:1-55);

k. using the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access (5:20-24).

36. Takeda '189 does not expressly disclose defining the associations. Stallings discloses an overview of PGP wherein one of the salient features of the invention defines an association between an encrypted data decryption key and a key-decrypting key, and between the encrypted data-decrypting key and the encrypted document, to efficiently identify which keys are sufficient to decrypt the encrypted document (pg. 365, figure 12.3). Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to define the key pair associations and the key/document associations for a more efficient means of identifying which keys decrypt which document. Stallings, pg. 363, last paragraph-pg. 364, first paragraph. The aforementioned cover the limitations of claim 26.

37. As per claims 27 and 28, the rejection of claim 26 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, in the abstract sense, the association of the key-decrypting key decrypting the encrypted data-decrypting key, which decrypts encrypted data defines a directed path, wherein decryption of the encrypted data requires the traversal of a path from a key-decrypting key to the encrypted data. Hence, claims 27 and 28 are covered by the teachings of Takeda '189 and Stallings.

38. As per claim 29, the rejection of claims 27 and 28 under 35 U.S.C. 103(a) are incorporated herein. (supra) In addition, each encrypted key is identified by two Ids, including a first ID corresponding to the encrypted key and a second ID corresponding to another of the keys capable of decrypting the encrypted key (Stallings, pg. 365, fig. 12.3: key ID of KUb identifies the key capable of decrypting the encrypted data-decrypting key, and the signature uniquely identifies the encrypted key and the encrypted message).

39. As per claim 35, it is a claim corresponding to claim 26 and it does not teach or define above the information claimed in claim 26. Therefore, claim 35 is rejected as being unpatentable over Takeda '189 in view of Stallings for the same reasons set forth in the rejection of claim 26.

Allowable Subject Matter

40. Claims 18-22, 30 and 31 are not covered by the prior art of record.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



August 17, 2005

Jung W Kim
Examiner
Art Unit 2132



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100